Amendments to the Claims

This listing of claims will replace all prior version and listings of claims in the application:

Listing of Claims:

1.   (Currently amended) A method of analyzing network communication traffic on a data communication network for determining whether the traffic is legitimate or potential suspicious activity, comprising the steps of:

monitoring packet headers of packets exchanged between two hosts on the data communication network;

based on the packet headers, determining the existence of identifying a client/server (C/S) flow as corresponding to a predetermined plurality of packets exchanged between the two hosts that relate to a single service and is characterized by a predetermined C/S flow characteristic;

assigning a concern index value to a determined C/S an identified flow based upon a predetermined concern index characteristic of the C/S flow;

maintaining an accumulated concern index comprising concern index values for one or more determined identified C/S flows associated with a host; and

issuing an alarm signal in the event that the accumulated concern index for a host exceeds an alarm threshold value.

2.   (Currently amended) The method of claim 1, wherein the predetermined C/S flow characteristic of a C/S flow is selected from the group comprising: the elapse of a predetermined period of time wherein no packets are exchanged between two hosts, the occurrence of a FIN flag, predetermined characteristics of traffic on a given port, and the occurrence of a RESET packet.

3.   (Previously presented) The method of claim 1, further comprising the step of
communicating a message to a firewall to drop packets going to or from the
particular host in response to the alarm signal.

4.   (Previously presented) The method of claim 1, wherein the alarm signal generates
a notification to a network administrator.

5.   (Currently amended) The method of claim 1, wherein each concern index value
associated with a predetermined concern index characteristic event is a
predetermined fixed value.

6.   (Currently amended) A method of analyzing network communication traffic on a
data communication network for determining whether the traffic is legitimate or
potential suspicious activity, comprising the steps of:

monitoring packet headers of packets exchanged between two
hosts that are associated with a single service on the data communications
network;

based on the packet headers, determining the existence of a
client/server (C/S) identifying a flow as corresponding to a predetermined
plurality of packets exchanged between the two hosts;

collecting C/S flow data from packet headers of the packets in the
determined identified flow;

based on the collected C/S flow data, assigning a concern index
value to the a determined C/S flow based on a predetermined concern
index characteristic of the C/S flow;

maintaining an accumulated concern index from C/S flows that are
associated with a particular host;

issuing an alarm signal in the event that the accumulated concern
index for the particular host exceeds an alarm threshold value; and

in response to the alarm signal, sending a message to a utilization

component.

7. (Previously presented) The method of claim 6, wherein the utilization component

is selected from the group comprising: network security device, email, SNMP

trap message, beeper, cellphone, firewall, network monitor, user interface display

to an operator.

8. (Currently amended) A method of analyzing network communication traffic on a

data communication network for determining whether the traffic is legitimate or

potential suspicious activity, comprising the steps of:

monitoring the packet headers from an exchange of packets

between two hosts each having a particular Internet Protocol (IP) address;

based on monitored packet headers, determining the existence of a

client/server (C/S) identifying a flow as corresponding to a predetermined

plurality of packets exchanged between a particular port of one of the

hosts that remains constant during the plurality of packets;

collecting C/S flow data from packet headers of the packets in a

determined C/S the identified flow;

based on the collected C/S flow data, assigning a concern index

value to the a determined C/S flow;

maintaining a host data structure containing accumulated concern

index values from a plurality of determined C/S flows that are associated

with the particular host; and

issuing an alarm in the event that the accumulated concern index

values for the particular host has exceeded an alarm threshold value.

9. (Previously presented) The method of claim 8, wherein each concern index value

associated with a respective potential suspicious activity is a predetermined fixed

value.

4

10.   (Currently amended) A system for analyzing network communication traffic and determining potential suspicious activity, comprising:

    a computer system operative to:

        a)   monitor <u>packet headers resulting from</u> the communication of packets on a data communication network;

        b)   <u>based on monitored packet headers</u>, classify the monitored packets into <u>client/server (C/S)</u> flows, wherein a <u>C/S</u> flow corresponds to a predetermined plurality of packets exchanged between two hosts that are associated with a single service on the network;

        c)   analyze the <u>C/S</u> flows in order to assign a concern index value to a <u>C/S</u> flow that may signify potential suspicious activity, wherein each concern index value associated with a respective potential suspicious activity is of a predetermined fixed value;

        d)   generate an alarm signal in response to cumulated concern index values; and

    a communication system coupled to the computer system operative to receive packets communicated between hosts on the network.

11.   (Currently amended) A system for analyzing network communication traffic and determining potential suspicious activity, comprising:

    a processor operative to:

        a)   monitor <u>packet headers resulting from</u> the communication of packets on a data communication network;

        b)   classify the monitored packets into <u>client/server (C/S)</u> flows, wherein a <u>C/S</u> flow corresponds to a predetermined plurality of packets exchanged between two hosts that are associated with a single service on the network;

c)   maintain a flow data structure for storing data corresponding to a plurality of C/S flows;

d)   analyze the C/S flows in the flow data structure in order to assign a concern index value to a C/S flow that may signify potential suspicious activity, wherein each concern index value associated with a respective potential suspicious activity is of a predetermined fixed value;

e)   cumulate assigned concern index values of one or more C/S flows associated with a particular host;

f)   maintain a host data structure for storing data associating a cumulated concern index value with each one of a plurality of hosts; and

g)   generate an alarm signal in response to cumulated concern index values in the host data structure;

a memory coupled to the processor and operative to store the flow data structure and the host data structure; and

a network interface coupled to the processor operative to receive packets on the data communication network.

12.   (Previously presented) A method of analyzing network communication traffic on a data communication network for potential suspicious activity, comprising the steps of:

monitoring packets exchanged between two hosts on the data communication network;

identifying packets provided by one of the two hosts that have a transport level protocol specifying a packet format that includes a data segment;

in response to determination that the transport level protocol is a User Datagram Protocol (UDP) packet and the data segment associated with the UDP packet contains two bytes or less of data, storing a concern

index value of a predetermined amount in a memory in association with

information identifying the host that issued the UDP packet; and

issuing an alarm when the cumulated concern index value

associated with the host exceeds a predetermined threshold level.

13. (Currently amended) The method of claim 6, wherein a C/S flow is characterized by a predetermined C/S flow characteristic selected from the group comprising: the elapse of predetermined period of time where no packets are exchanged between two hosts, the occurrence of a FIN flag, predetermined characteristics of traffic on a given port, and the occurrence of a RESET packet.

14. (Currently amended) The method of claim 8, wherein a C/S flow is characterized by a predetermined C/S flow characteristic selected from the group comprising: the elapse of a predetermined period of time wherein no packets are exchanged between two hosts, the occurrence of a FIN flag, predetermined characteristics of traffic on a given port, and the occurrence of a RESET packet.

15. (Currently amended) The system of claim 10, wherein a C/S flow is characterized by a predetermined C/S flow characteristic selected from the group comprising: the elapse of a predetermined period of time wherein no packets are exchanged between two hosts, the occurrence of a FIN flag, predetermined characteristics of traffic on a given port, and the occurrence of a RESET packet.

16. (Currently amended) The system of claim 11, wherein a C/S flow is characterized by a predetermined C/S flow characteristic selected from the group comprising: the elapse of a predetermined period of time wherein no packets are exchanged between two hosts, the occurrence of a FIN flag, predetermined characteristics of traffic on a given port, and the occurrence of a RESET packet.

17. (Previously presented) The method of claim 1, wherein the single service comprises a port number remaining constant for a plurality of packets.

18.   (Previously presented) The method of claim 1, wherein the suspicious activity is from an inside address or from an outside address.

19.   (Previously presented) The method of claim 1, wherein the concern index for a suspicious activity is derived by reference to a table of predetermined suspicious activities each having a predetermined concern index value.

20.   (Previously presented) The method of claim 1, wherein the host for which the concern index is accumulated is an inside host.

21.   (Previously presented)   The method of claim 1, wherein the host for which the concern index is accumulated is an outside host.

22.   (Previously presented) The method of claim 1, wherein the steps are carried out in a monitoring appliance.

23.   (Previously presented) The method of claim 22, wherein the monitoring appliance is installed behind a firewall.

24.   (Previously presented) The method of claim 22, wherein the monitoring appliance is connected before a firewall.

25.   (Previously presented) The method of claim 22, wherein the monitoring appliance is connected in a DMZ.

26.   (Previously presented) The method of claim 22, wherein the monitoring appliance is configured to operate as a pass-by filter.

27.   (Previously presented) The method of claim 22, wherein the monitoring
        appliance is coupled to a network device.

28.   (Previously presented) The method of claim 27, wherein the network device is
        selected from group comprising: router, switch, hub, tap.

29.   (Previously presented) The method of claim 27, wherein the network device is a
        network security device.

30.   (Previously presented) The method of claim 1, wherein the monitoring of packets
        comprises monitoring on packet header information only.

31.   (Previously presented) The method of claim 1, wherein the monitoring of packets
        is carried out in a device operating in a promiscuous mode.

32.   (Previously presented) The method of claim 1, wherein the alarm signal is
        provided to a utilization component.

33.   (Previously presented) The method of claim 32, wherein the utilization
        component is selected from the group comprising: network security device,
        email, SNMP trap message, beeper, cellphone, firewall, network monitor, user
        interface display to an operator.

34.   (**New**) The method of claim 1, wherein the predetermined concern index
        characteristic comprises a characteristic selected from a table comprising a
        plurality of prestored second predetermined characteristics each having a
        predetermined concern index (CI) value.

35.   (**New**) The method of claim 1, wherein the predetermined concern index
        characteristic comprises one or more of the following characteristics: potential

TCP probe, potential UDP probe, half-open attack, TCP stealth port scan, UDP

stealth port scan, bad flags, short UDP, address scan, port scan.

36.   (**New**) The method of claim 6, wherein the predetermined concern index

characteristic comprises a characteristic selected from a table comprising a

plurality of prestored second predetermined characteristics each having a

predetermined concern index (CI) value.

37.   (**New**) The method of claim 6, wherein the predetermined concern index

characteristic comprises one or more of the following characteristics: potential